



ATTORNEY GENERAL ROY COOPER
North Carolina Department of Justice

A RESOURCE GUIDE FOR TEACHERS
AND SCHOOL RESOURCE OFFICERS

INTERNET

SAFETY

**WHAT YOU DON'T KNOW
CAN HURT YOUR STUDENTS**



ACKNOWLEDGEMENTS

Many individuals helped make this Internet safety project possible. We would like to particularly thank Gail Barnes, John Bason, Jay Chaudhuri, Lauren Chen, Caroline Farmer, Noelle Talley, Julia White, and Carol Young of the North Carolina Department of Justice; and Special Agent Kevin West of the North Carolina State Bureau of Investigation and the North Carolina Internet Crimes Against Children Task Force; Nancy McBride of the National Center for Missing & Exploited Children; Eddie Davis of the North Carolina Association of Educators; Martha Campbell of the North Carolina Department of Public Instruction; Tom Williams of the Granville County Public Schools; Amy Washburn Cheney of the Union County Public Schools; and Professor Tony Brock of the Department of Graphic Design at North Carolina State University.

This project was supported by federal formula grant project # 2003-IJ-CX-K019, awarded by the Office of Justice Programs, United States Department of Justice. Points of view or opinions contained within this document are those of the authors and do not necessarily represent the official position or policies of the United States Department of Justice.



A total of 6,000 copies of this public document were printed by the North Carolina Department of Justice at a cost of \$7,828 or \$1.30 per copy. These figures include only the direct costs of reproduction. They do not include preparation, handling, or distribution costs.

COPYRIGHTED LOGOS OR IMAGES CONTAINED IN THIS DOCUMENT ARE USED FOR EDUCATIONAL PURPOSES ONLY AND ARE THE PROPERTY OF THE COPYRIGHT OWNER. THEIR USE DOES NOT IMPLY ENDORSEMENT OF THE MATERIAL IN THIS DOCUMENT BY THE COPYRIGHT OWNER, NOR DOES IT IMPLY ENDORSEMENT OF ANY COMPANY OR ITS PRODUCTS BY THE NORTH CAROLINA DEPARTMENT OF JUSTICE.

COMPUTERS AND THE INTERNET HAVE REVOLUTIONIZED THE WAY WE WORK, SHOP, AND EDUCATE STUDENTS. BUT ALONG WITH THE POSITIVE CHANGES COME NEW RESPONSIBILITIES AND POTENTIAL DANGERS. HAZARDS THAT BEGIN WITH INNOCENT COMPUTER USE CAN THREATEN THE SAFETY AND WELL-BEING OF STUDENTS UNDER YOUR CARE.

For example, child predators who cruise the playgrounds for victims now spend time cruising the Internet. In fact, a survey found that one out of every five young Internet users said that they had received an unwanted sexual solicitation online in the past year.

Educators have a responsibility to protect students when they are in school. This resource guide and the video that accompanies it are designed to help teachers and School Resource Officers learn about the steps they can take to protect students, and the resources that are available to them.

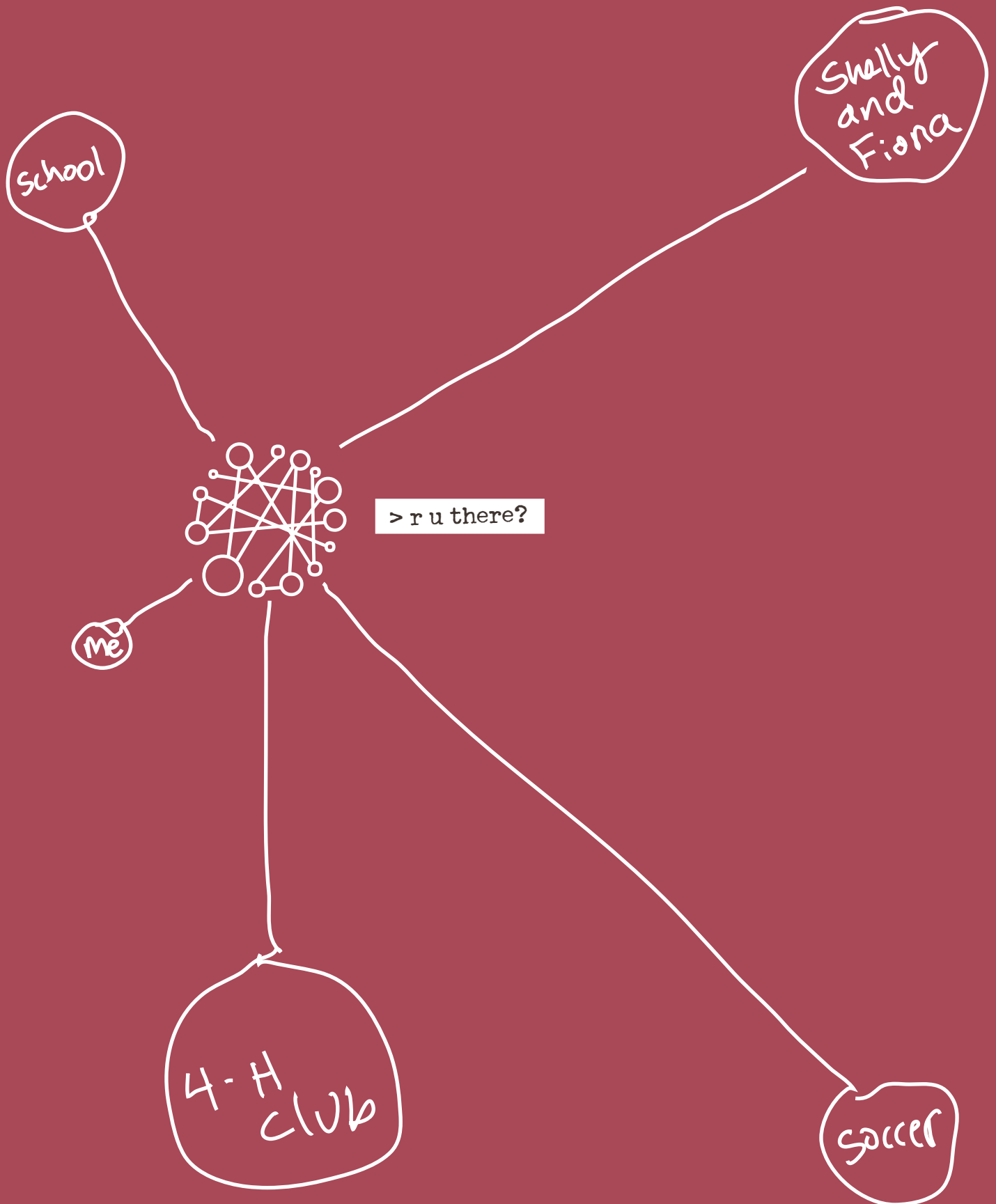
Just as you might supervise your students when they are learning to drive a car during driver education, you need to guide and monitor your students' use of the Internet. A child can get into serious trouble sitting in front of a computer screen, right under your nose. The most important thing a teacher can do when working with students who are using computers is to **PHYSICALLY MONITOR STUDENTS' ONLINE ACTIVITY.**

Your school's door may be locked against intruders, but if your computers aren't properly secured and used safely, they can be an open window to people who seek to exploit and harm young people. They can threaten the safety of the children who have been placed in your care... your students.

A handwritten signature in dark ink, reading "Roy Cooper". The signature is stylized, with the first name "Roy" and the last name "Cooper" written in a cursive-like script.

Roy Cooper
Attorney General





6

BACKGROUND

Online Risks for Children
Child Predators
Assessing Dangers at School

19

ONLINE DANGERS COME TO SCHOOL

20

THREATS VIA ELECTRONIC COMMUNICATION

24

PORNOGRAPHY ON SCHOOL COMPUTERS

26

ADDITIONAL INFORMATION FOR EDUCATORS

Monitor the Monitors
School Website Safety
The Password is . . . Secret
What's in a Domain Name?
Avoid "Surprising" Search Results

32

APPENDIX

For School Resource Officers: Email Headers

In some instances, procedures suggested in this guide may be in conflict with policies at your school or school district. In such cases, follow your school or district's procedures first, and then consider taking additional steps that may be outlined in this guide.

NOTE: THIS PUBLICATION USES THE TERM "CHILD PREDATOR" AS A CONVENIENT WAY TO REFER TO AN ADULT WHO SEEKS CHILDREN. HOWEVER, EXPERTS WARN THAT THE STEREOTYPE OF A CHILD PREDATOR (FOR EXAMPLE, A SUSPICIOUS-LOOKING MAN WEARING A TRENCH COAT) IS INACCURATE. PARENTS AND EDUCATORS SHOULD BE AWARE THAT ANY ADULT COULD BE SOMEONE WHO WOULD EXPLOIT A CHILD.

SOME VISITORS DON'T WALK THROUGH THE

FRONT DOOR

OR SIGN IN AT THE OFFICE.

ADULTS WHO WANT TO

EXPLOIT

YOUNG PEOPLE CAN ENTER

YOUR SCHOOL

THROUGH THE

INTERNET

>LMIRL @ 3:15. ttyl :o)



1 in 5 youths between the ages
of 10 and 17 has received
unwanted sexual solicitations online¹

1 in 4 youths has been exposed
to sexually explicit pictures
online without seeking
or expecting them¹

1 in 17 youths has been
threatened or harassed online¹

1 in 33 youths has received
an aggressive solicitation
to meet somewhere¹

ONLINE RISKS FOR CHILDREN

Millions of children under the age of 18 use the Internet, and the number of children who are spending time online has increased significantly in recent years.² This relatively new communication tool presents a variety of risks for these children.

They include:

SOLICITATIONS BY CHILD PREDATOR

Most North Carolina parents (60%) felt their children are at some risk of being contacted or preyed upon by someone they do not know while on the Internet.³

UNWANTED EXPOSURE TO SEXUAL MATERIAL

Most North Carolina parents (80%) expressed concern about sexually explicit materials on the Internet.³

THREATS OR HARASSMENT ONLINE

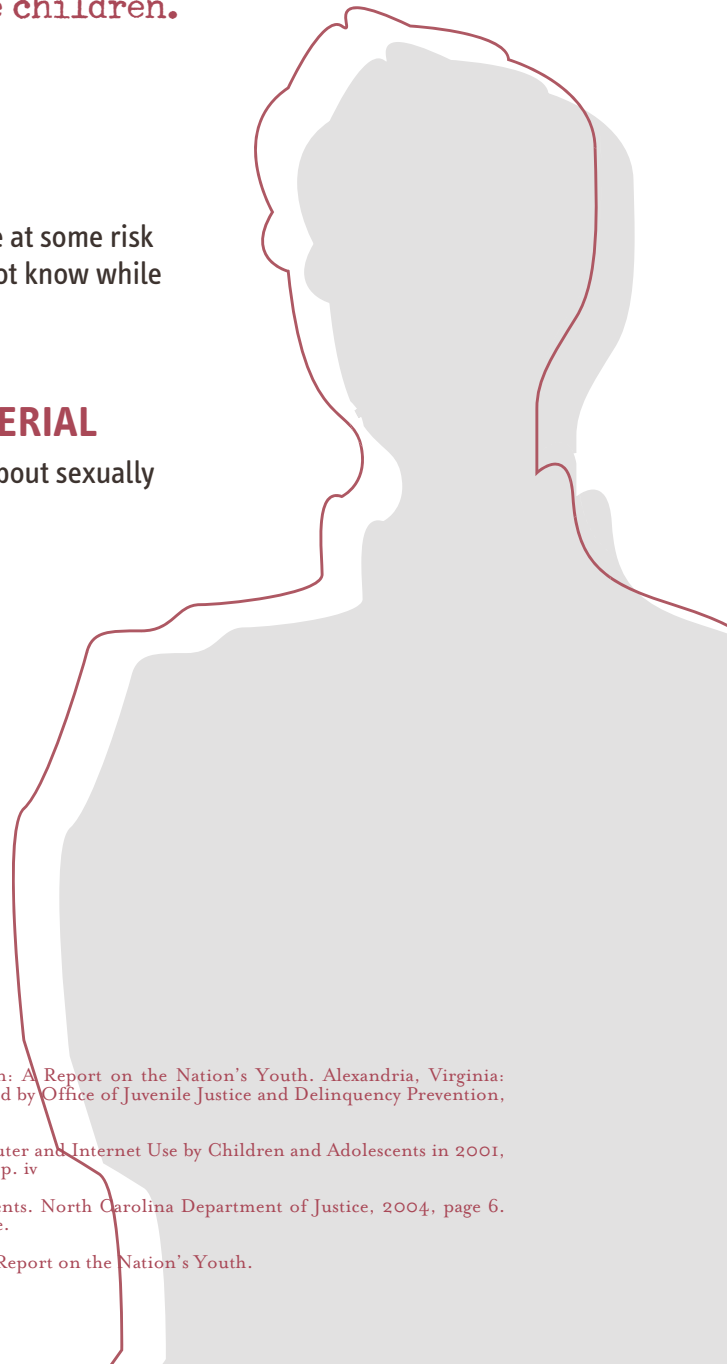
Only about half of the children who were threatened or harassed reported the incident to their parents.⁴

1. David Finkelhor, Kimberly J. Mitchell, and Janis Wolak. Online Victimization: A Report on the Nation's Youth. Alexandria, Virginia: National Center for Missing & Exploited Children, 2000, page ix. Funding provided by Office of Juvenile Justice and Delinquency Prevention, United States Department of Justice.

2. U.S. Department of Education, National Center for Education Statistics, Computer and Internet Use by Children and Adolescents in 2001, NCES 2004-014, by Matthew DeBell and Chris Chapman. Washington, DC: 2003, p. iv

3. Children's Internet Use: An Online Survey of Concerned North Carolina Parents. North Carolina Department of Justice, 2004, page 6. Funding provided by Office of Justice Programs, United States Department of Justice.

4. David Finkelhor, Kimberly J. Mitchell, and Janis Wolak. Online Victimization: A Report on the Nation's Youth.





The Internet makes it easy for predators to locate potential victims and communicate with them. Ultimately, they want to lure children to a face-to-face meeting. That's why it is important to understand how children are targeted by adults who want to exploit them.

the Internet
makes it

EASY
for predators
to locate



POTENTIAL VICTIMS



anonymity. For some teens
they feel safe in front of a computer.
observe, approach, and then groom

A **CHAT ROOM** is a place online where
messages are usually displayed

all at once on their computer screen.
looking for a child victim in North

The search for a potential victim frequently begins in a chat room. A **CHAT ROOM** is a place online where people can go to “talk” with each other by typing messages. These messages are usually displayed almost instantly.

Those in the chat room can view all of the conversations taking place at once on their computer screen. Chat rooms may be divided into categories. For example, an adult looking for a child victim in North Carolina may visit a “North Carolina” chat room for teenagers.



COMMUNICATION AND “GROOMING”

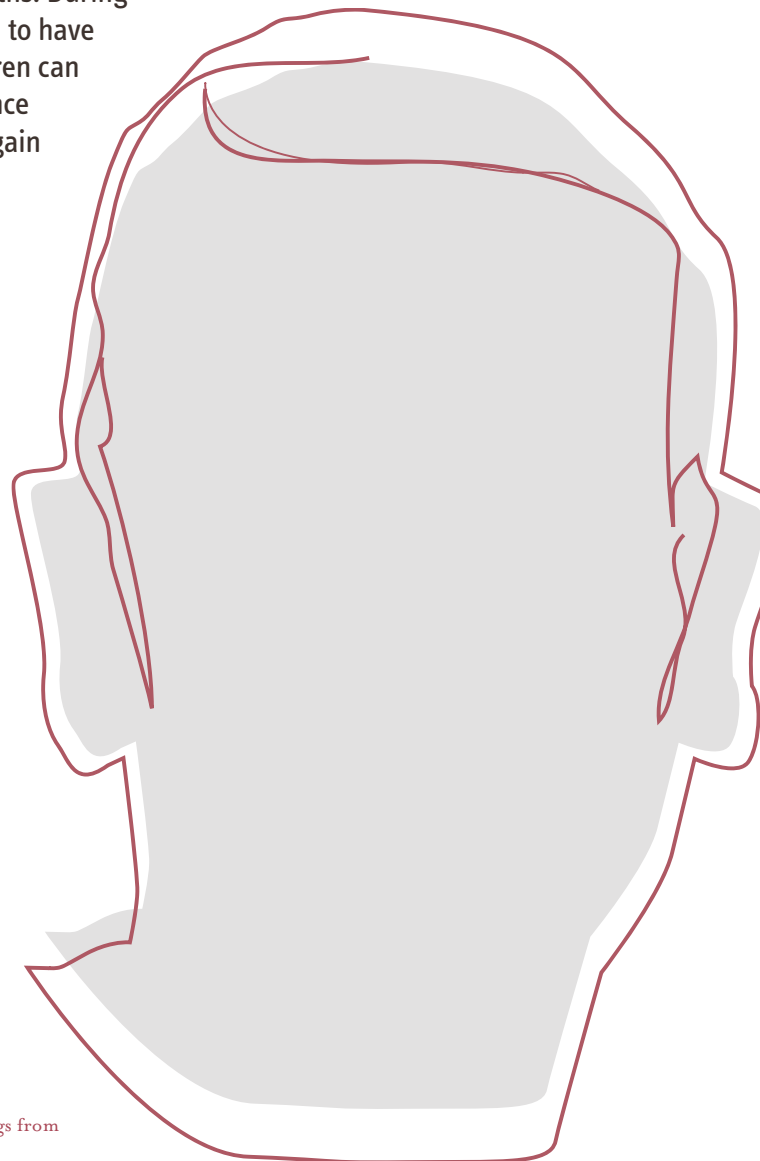
Predators may use email, instant messaging, and other methods to communicate with a child. **EMAIL** is a method of sending messages electronically from one computer to another. **INSTANT MESSAGING** (IM) is a service that alerts users when friends are online and allows them to communicate with each other in real time through private online chat areas.

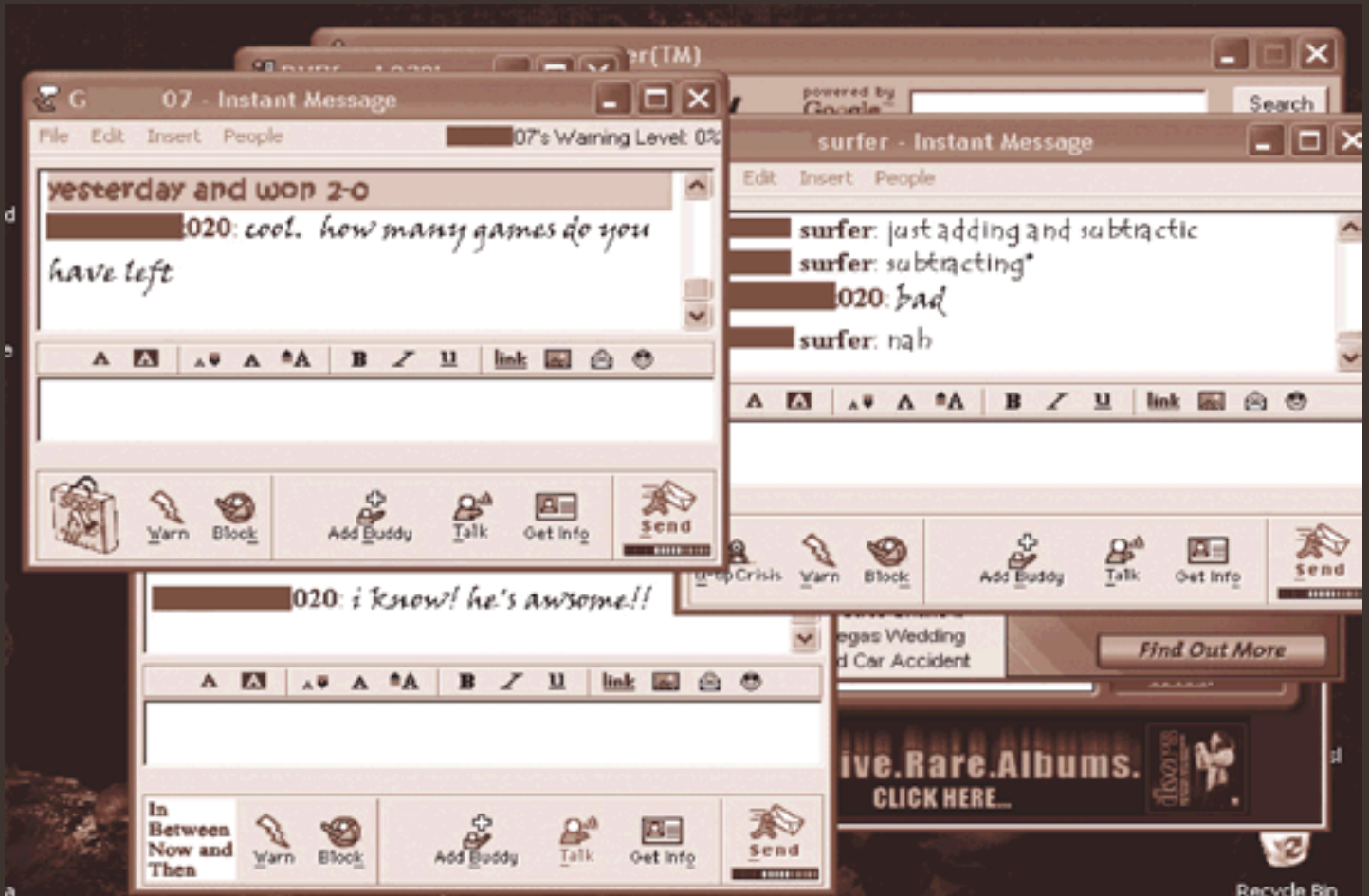
When an online predator targets a child, he engages in a grooming process that can take anywhere from a few weeks to several months. During this period, he will sympathize with the child and pretend to have similar interests. Adults who are seeking to exploit children can be extremely convincing. They also rely on the inexperience of their potential victims, knowing what to say and do to gain their trust.

The grooming process frequently ends with an attempt to meet a child outside of the home. A recent study found that most children who agree to meet face-to-face with an adult do so willingly. They are not tricked or coerced.⁵

To learn more about the grooming process, visit WWW.NCDOJ.COM. Under the Jump To menu, select “Internet Safety” and then “Parents and Guardians.” See “Online Predators” and “The Grooming Process.”

5. David Finkelhor, Kimberly J. Mitchell, and Janis Wolak. Internet-Initiated Sex Crimes Against Minors: Implications for Prevention Based on Findings from a National Study. *Journal of Adolescent Health*, 2004, volume 35, page 11.





This illustration shows multiple IM sessions.

These are actual instant messages; screen names have been blocked.

TTYL

CHAT ROOM AND INSTANT MESSAGE ABBREVIATIONS

Young people have developed many keyboard shortcuts to save time. These abbreviations also keep adults from knowing what they are saying. Here are a few examples:

DIKU —————> Do I know you?

A/S/L —————> Age/Sex/Location?

LMIRL —————> Let's meet in real life

TAW —————> Teachers are watching

KWIM

10101010001110001010100001 1010101111001010100100101010 1010100010101010100101000111001010100010101010100101010001110010101

For more examples of chat
abbreviations, visit
WWW.NCDOJ.COM



Under the Jump To menu, select "Internet Safety."
Click on "Educators" and then
"Additional Resources for Educators."

See the listing for the National Center for
Missing & Exploited Children.

ASSESSING DANGERS AT SCHOOL

Educators and School Resource Officers spend a significant amount of time with students. For the most part, your interactions with these young people might be described as routine.

However, in the course of a school day you may learn of situations that could threaten the safety of students.

This information can come from a variety of sources, including:

intercepted notes or messages

overheard conversations

tips from students

personal observation

In any situation, you must use your training and experience to decide how you should respond to the information. The North Carolina Department of Public Instruction has developed guidelines that can assist school personnel.

To view the DPI brochure “An Educator’s Guide for Prevention and Early Intervention,” visit ncdoj.com. Under the Jump To menu, select “Internet Safety.” Locate “Additional Resources for Educators” and look under “Publications.”

HAS YOUR SCHOOL PREPARED ITS CRITICAL INCIDENT RESPONSE KIT?

Educators must work to prevent potential problems, but they must also know how to react appropriately if problems occur. All North Carolina schools have received a copy of the video “A Critical Incident: What To Do In The First Twenty Minutes” and its accompanying resource guide.

These materials are designed to prepare school personnel for a worst-case scenario, like a school shooting. For more information about the Critical Incident Response Kit program, visit www.ncdoj.com and click on “Protecting Children.”





ONLINE DANGERS COME TO SCHOOL

In the video “Internet Safety: What You Don’t Know Can Hurt Your Students,”* a teacher becomes suspicious when she witnesses a student hesitate before ultimately getting into a car outside the school.

After discovering that the student did not have permission to leave campus, the teacher immediately contacts law enforcement.

APPROPRIATE RESPONSE

WHEN A CHILD MAY BE IN DANGER, ACT QUICKLY

If you learn that a child may be in danger or is missing under suspicious circumstances, don’t hesitate to act.

CONTACT LAW ENFORCEMENT

When a child is missing or may be in danger, authority figures should contact law enforcement immediately. If your school has a School Resource Officer (SRO), the first step should be to contact that officer. If your school doesn’t have an SRO, contact local law enforcement.

DON’T SEARCH A COMPUTER UNLESS INSTRUCTED BY LAW ENFORCEMENT

In the video, a teacher suspects that a computer may have played a role in a student’s unauthorized departure from campus. In these situations, you’ll need to consider your next step carefully. Preserving potential evidence in a computer is a top priority.

Under certain circumstances, when fast reaction is critical but experts have not arrived, you may be instructed by law enforcement to immediately search a computer for clues. As a general rule, you should not undertake a search of a computer without first contacting law enforcement and getting their recommendation on whether to proceed.

* The video “Internet Safety: What You Don’t Know Can Hurt Your Students” is available by request and via streaming video at www.ncdoj.com.

In the video “Internet Safety: What You Don’t Know Can Hurt Your Students,” a student receives a threat online and approaches a teacher for help.

After the teacher accesses the threatening email, she immediately contacts her school’s SRO.

THREATS VIA ELECTRONIC COMMUNICATION

Email, instant messaging, chatting, and text messaging are useful communication tools, but they also provide a convenient method for delivering anonymous threats.

Teachers and SROs who become aware of such threats must decide whether the message represents an imminent danger. If so, appropriate actions must be taken.

SCHOOLS CAN HANDLE MANY THREATS

If the identity of the person who is making the threats can be determined and school officials believe there is no danger of imminent harm, they may be able to handle the threat administratively. In most cases, harassment and online bullying can be addressed in this manner.

NOTIFY LAW ENFORCEMENT OF SERIOUS THREATS, IMMINENT DANGER

If the identity of the person who is making the threats cannot be determined or there is danger of imminent harm, law enforcement should be notified. This is a judgment call on the part of school authorities. If you are unsure about a situation, remember it is better to err on the side of caution and report a threat to law enforcement than put someone’s safety at risk.

FORWARD THE ENTIRE MESSAGE

When law enforcement officials are not on the scene but need to view a threatening email, forward the original message. Do not fax the printed email or “cut and paste” the body of the message into another email. Email messages include routing data, known as **HEADERS**. Headers can provide information to investigators, including the name of the person who originally sent the message.

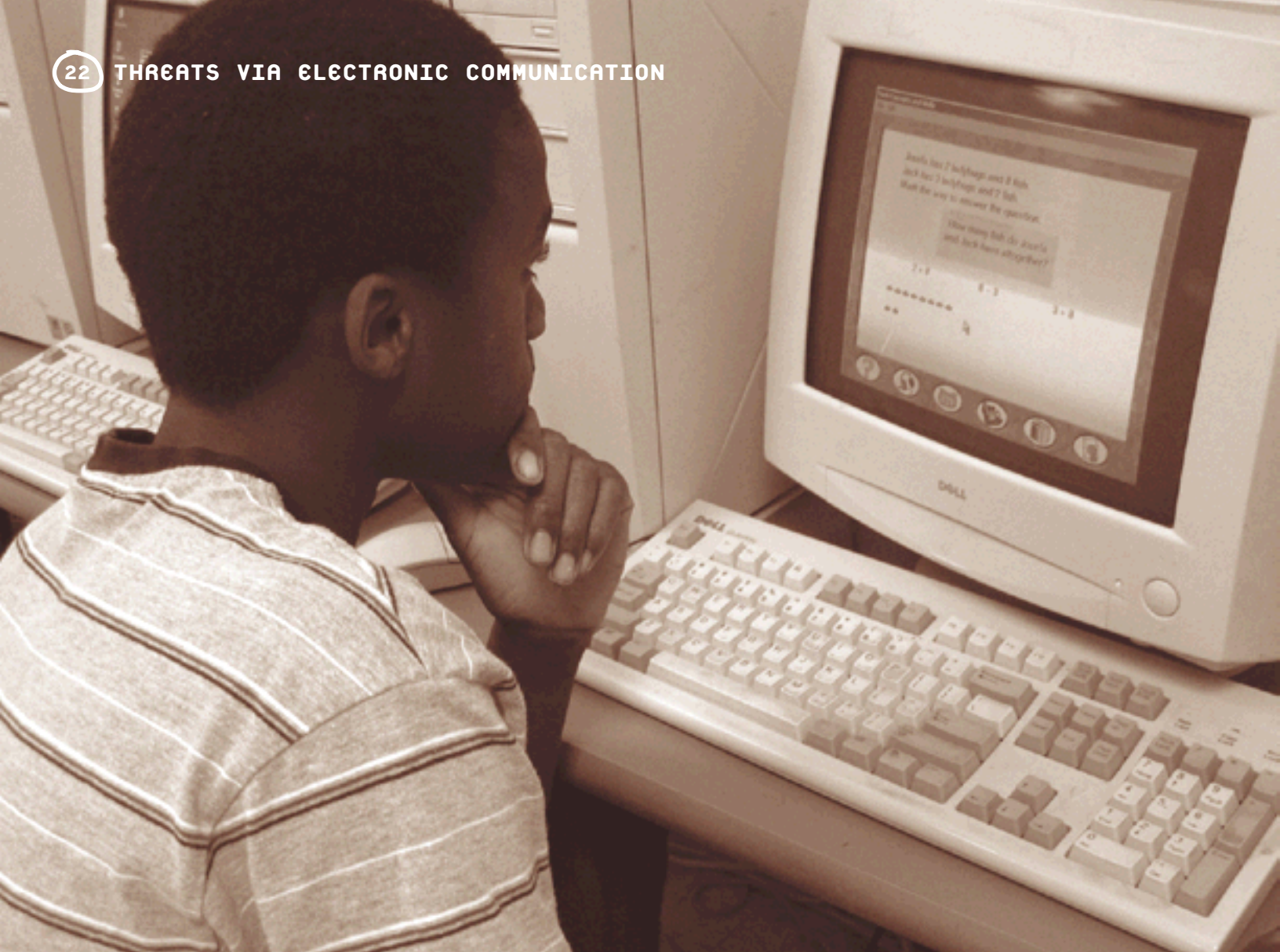
In many cases, forwarding the original message to law enforcement will make the headers available for their inspection. However, some email programs will not forward the headers along with the original message. If law enforcement does not receive the headers, they may be able to assist you in accessing and forwarding header information.

It is better to err
on the side of
CAUTION

and report a **THREAT**
to law enforcement
than put someone's



SAFETY AT RISK



It doesn't take a computer expert to examine email headers, but it does take someone who has received specialized training. This training is available to North Carolina law enforcement officers in the course "Fundamentals of Cybercrime Investigation" offered by the North Carolina Justice Academy.

For more information, visit the Academy on the web at WWW.JUS.STATE.NC.US/NCJA.

Officers who have previously received email header training will find helpful information in the Appendix of this publication. Additional information and resources are also available at WWW.NCDOJ.COM. Under the Jump To menu select "Internet Safety," then click "Additional Resources."

Email at school

School policies regarding the use of student email vary by school district. Some districts prohibit it, while others allow it if parents provide written permission for their child to use email.

Most schools permit the use of email, chat, or instant messaging only for curricular activities and under the direct supervision of a teacher.

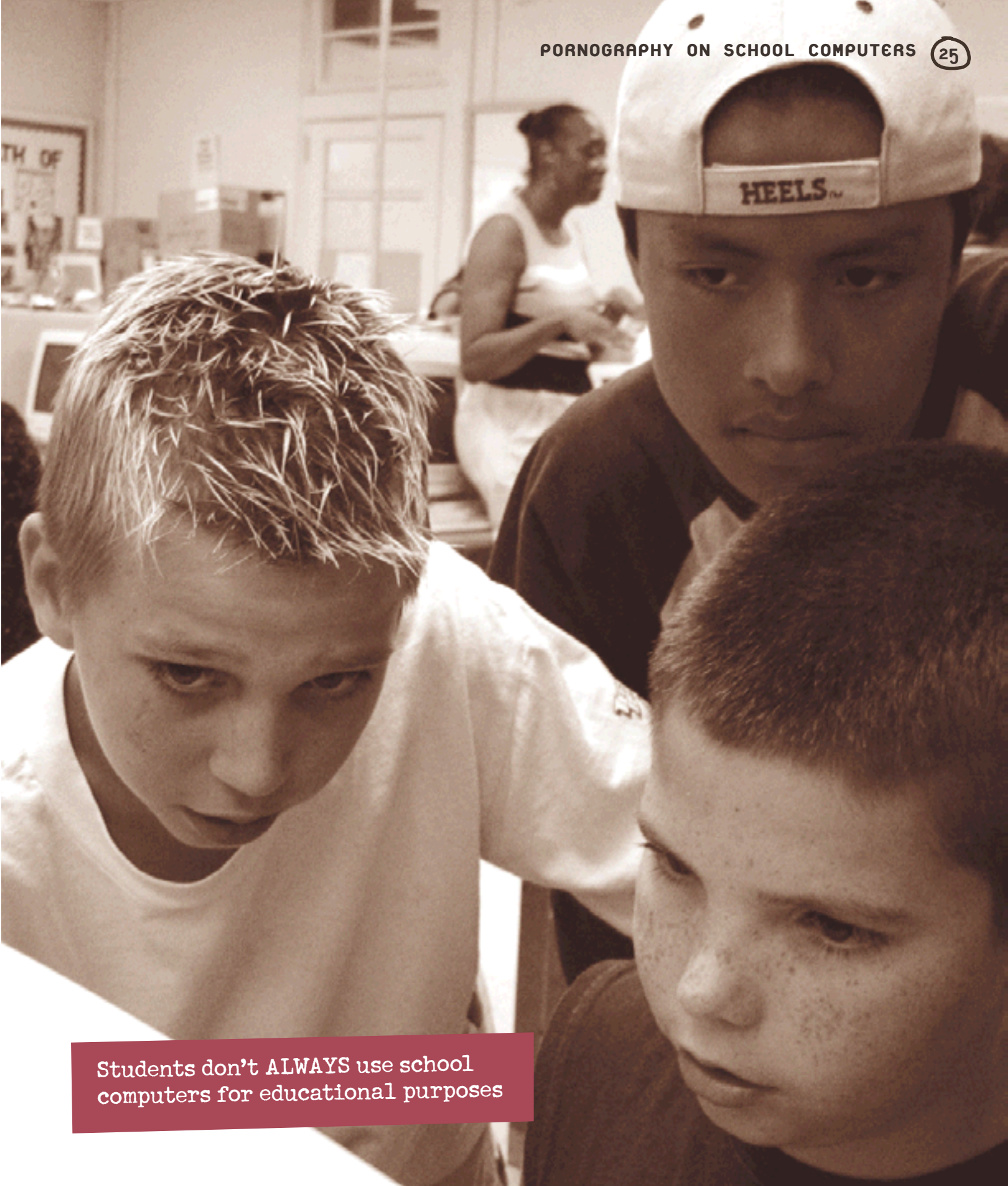
Districts that allow students to access email can take advantage of systems that limit how email is used. For example, Think.com and Gaggles.net offer free web-based email for schools.

greenville13@think.com

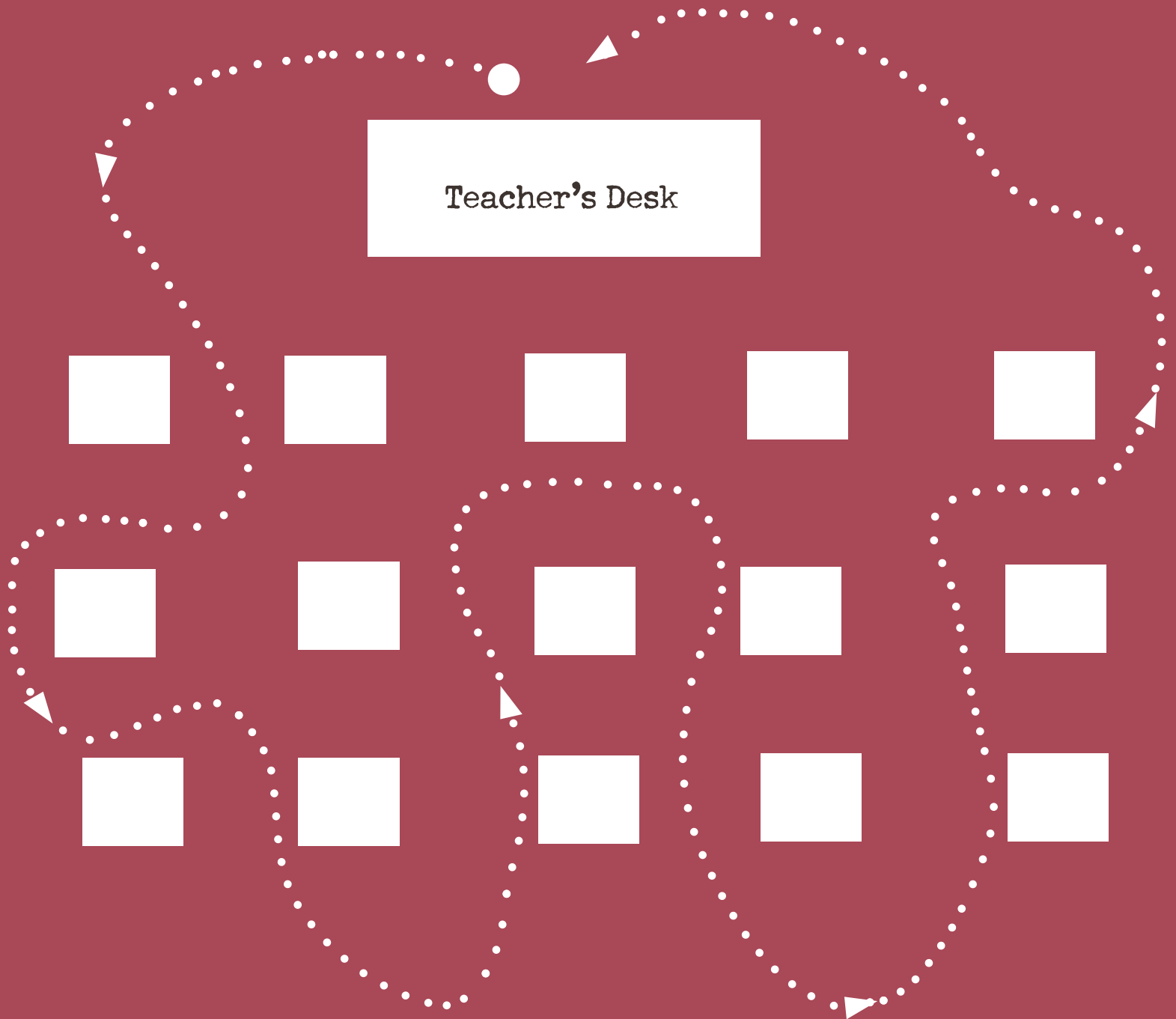
[illegible]

After discovering that the students have used the computer to access pornography on the Internet, she contacts the principal.

If the child pornography is a picture of a student, the most immediate concern is for the safety of the child. In this instance, local authorities should be contacted without delay.



Students don't ALWAYS use school computers for educational purposes



WALK AROUND THE CLASSROOM.

Look at your students' monitors.

ADDITIONAL INFORMATION FOR EDUCATORS

THE MOST IMPORTANT THING A TEACHER CAN DO WHEN WORKING WITH STUDENTS WHO ARE USING COMPUTERS IS TO PHYSICALLY MONITOR STUDENTS' ONLINE ACTIVITY. GET UP AND WALK AROUND THE CLASSROOM SO THAT YOU CAN VIEW STUDENTS' MONITORS.

MONITOR THE MONITORS

Filtering and monitoring software can provide a false sense of security. They are no match for your personal observation of students. Let students know that you are watching and that they are expected to obey the rules for using school computers. Students should understand that there are consequences for inappropriate use of their school's technology. Fear of being caught "out of bounds" is a strong deterrent to student misuse of school computers.

HINT: when possible, configure computer labs so every computer monitor can be seen from a single vantage point.

SCHOOL WEBSITE SAFETY

The Internet is a great way to highlight the good work done at your school, but be careful how it is used. Avoid posting photographs of individual students. If students are depicted, they should be seen in group photos, at a distance. Never post any identifying information about a student, such as their name or address, on a school website or in an electronic newsletter.

THE PASSWORD IS ... SECRET

Keeping your password secure is an essential element of safer computer use. Security experts say that far too often computer users leave their passwords in plain sight. In fact, a school visitor once found a computer username and password posted on the edge of a computer monitor at the desk of a School Resource Officer.

Students who use computers at school should have their own individual password or login to gain access to a computer. They should not share their passwords with anyone. School employees and staff should lead by example. Don't leave your password where someone who glances at your desk or opens your desk drawers can find it.

WHAT'S IN A DOMAIN NAME?

With so much inappropriate material online, the Internet can be a frightening place for educators who are entrusted with the care of young minds.

Teachers who are hesitant to direct their students online can count on a few things:

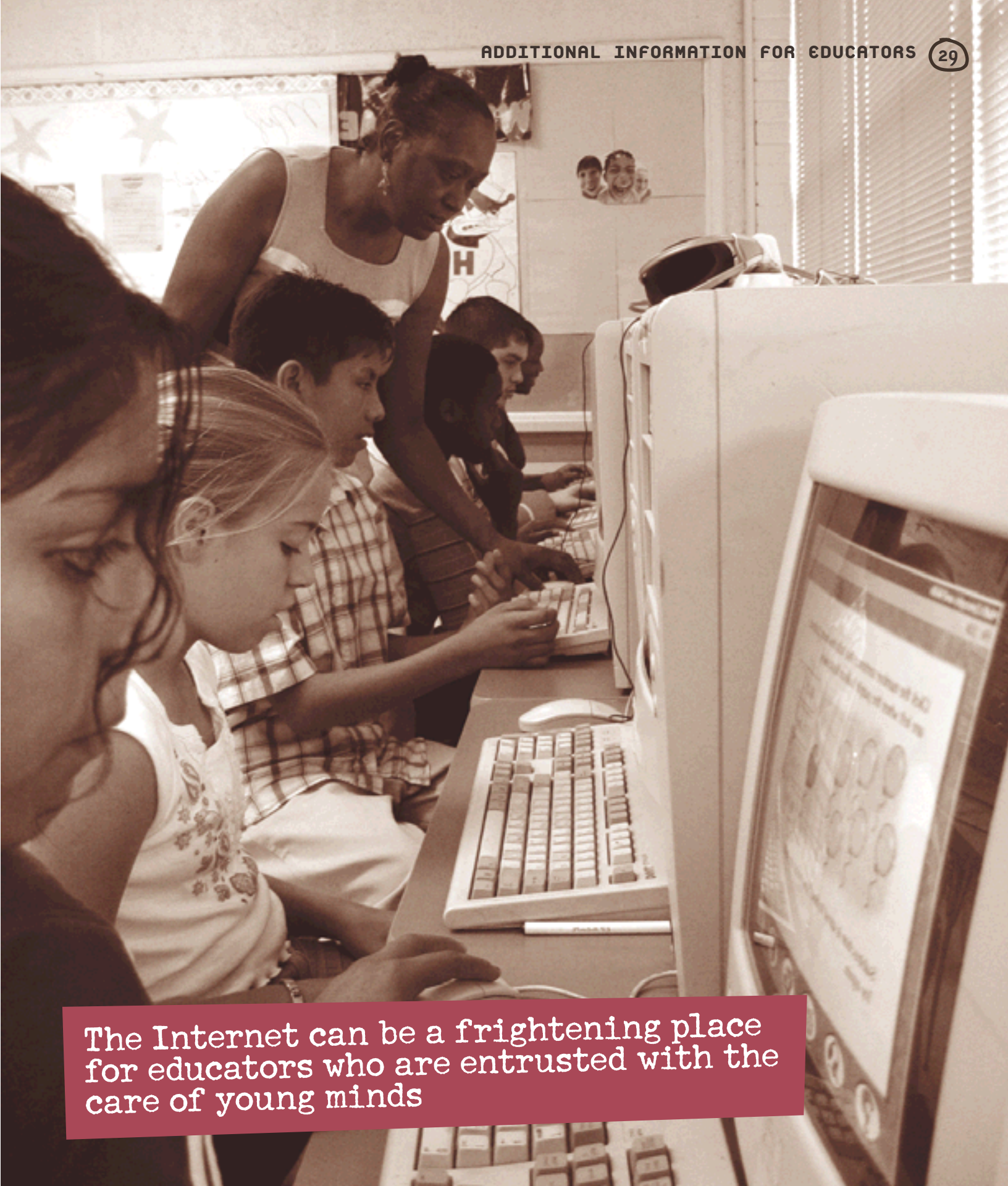
- Any domain name that ends in **.GOV** is a government website and unlikely to contain material that is inappropriate for young people.
- Likewise, any domain name that ends in **.EDU** is a website affiliated with an educational facility and unlikely to contain any inappropriate material.
- On the other hand, you take your chances with **.COM**, **.ORG**, or **.NET** websites. Most are suitable, but many are not.

Some web safety advocates are lobbying for the creation of a **.xxx** domain name for adult-oriented websites. But even if a **.xxx** domain name is established, it is believed that many adult-themed sites will remain at their current addresses.

WHAT'S IN A DOMAIN NAME, PART II: SEEING IS BELIEVING

For an example of how important a domain name can be, visit whitehouse.gov. This is the official website of the United States President.

If you were to replace **.gov** with one of the other domain names, you might find a parody of the official White House website, a billboard of links to inoffensive material, or even links to pornography. Visit one of these sites again a few months later, and it may have changed into something completely different. Such is the nature of the Internet. But that is also why domain names that end in **.gov** and **.edu** are so helpful to educators.



The Internet can be a frightening place for educators who are entrusted with the care of young minds

Utilizing AGE-APPROPRIATE search engines
permits **SAFER** online research
at school,
the public library,
or home



HOW TO BOOKMARK

To bookmark a website, access the site you want and then go to your web browser's toolbar. If you are using Internet Explorer, click on "Favorites" near the top of the page. When that menu appears, click "Add To Favorites."

Other browsers may use a term like "Bookmark This Site," but the result is the same: you save the site for easy access. When it is time to do the research, students just click on the saved link.

Note: Due to the changing nature of the Internet, educators should re-check websites that were bookmarked in the past to make sure their content is still appropriate before directing students to those sites.

AVOID “SURPRISING” SEARCH RESULTS

Internet searches can sometimes lead to unexpected search results. But there are a number of ways for teachers to help their students use the Internet without exposing them to inappropriate material. In the first two methods listed below, students do not conduct web searches. In the third method students conduct web searches, but they use search engines that limit the results of their searches.

1) Give students specific web addresses

This method takes students to a specific place on the Internet. Supplying students with a precise web address works for web research conducted at school, the public library, or home.

2) Use bookmarks

In this method, students access pre-determined web pages by clicking links that a teacher has loaded onto the classroom's computers. The process of pre-loading Internet browsers with links is called “bookmarking.” This method only works for research at school.

3) Direct students to age-appropriate search engines

This method allows you to help students learn about Internet research while significantly reducing the possibility of exposure to inappropriate material. Utilizing age-appropriate search engines permits safer online research at school, the public library, or home.

Age-appropriate search engines include:

Learn NC (learnnc.org/bestweb) - Learn NC's “Best of the Web” collection provides a searchable, annotated catalog of more than 3,000 educational websites.

Kidsclick (kidsclick.org) - Created by librarians to guide young users to age-appropriate websites.

Ask Jeeves for Kids (ajkids.com) - A site focused on learning.

Yahooligans (Yahooligans.Yahoo.com) - The Yahoo web guide for kids.

APPENDIX:

INFORMATION FOR SCHOOL RESOURCE OFFICERS

Email Headers

Don't search a computer unless you are sure that you will not cause harm to the information it contains. This is true of email as well.

There is data attached to email that can sometimes offer clues about the sender. A person who has received the proper training may be able to look at this data and gather helpful information about the sender, without causing harm to the message.

HEADER CAN REVEAL EMAIL SENDER

Emails have hidden routing information (called a "header") that shows the trail that the message took on the way to its intended recipient. The header also indicates the name of the sender.

SAMPLE HEADER



```
Received: from siemms01
(mail.jus.state.nc.us [1299.90.253.53])
by ncdoj.com; Mon, 15 Nov 2004 08:48:29 -0500
Received: from bronz.hexwea.com (10.1.543.39) by Sigaba.hexwea.com
(Sigaba Gateway v3.6.1) with ESMTP id 21663892; Mon, 15 Nov 2004 08:53:51
-0500
X-SEF-BDEFCA37-3511-4818-A318-B3AAA19F080: 1
Received: from Charles Baker [10.1.53.23] by bonzaimf.hexwea.com - SurfControl
E-mail Filter (5.0); Mon, 15 Nov 2004 08:53:51 -0500
Received: by thinman1.hexwea.com with Internet Mail Service
(5.5.2657.72) id <VLQWPDHB>; Mon, 15 Nov 2004 08:53:51 -0500
Message-ID: <A8A654504741EA47A6BF2BAA90FBD3440D7C7453@thinman1.hexwea.com>
```

The information in a header can be particularly helpful in cases where a person who has been receiving threats does not know who is sending them.

However, not everything in an email can be taken at face value. Some computer users are skillful enough to use the name of an innocent third party or hide behind a false name. But others may not be as skillful. In those cases, it may be possible to pinpoint the sender of a particular email by studying the header.

DIFFERENT EMAIL SOFTWARE = DIFFERENT LOCATION OF HEADER INFORMATION


Many types of software are used to send and receive email on the Internet. Different email systems encode headers in different ways. When an email is forwarded, some email software programs include the header information along with the message. However, other email software programs do not include headers when a message is forwarded. In those instances, the assistance of an officer who has received computer crimes investigation training will be needed in order to access headers.

Officers who have received training on email headers will find helpful information about examining the headers of a particular email message at WWW.NCDOJ.COM.

Under the Jump To menu, click on “Internet Safety.” Visit the “Law Enforcement and Prosecutors” page and click on “Additional Resources.” Then click on the link under Headers to receive specific information about how to access the header of the email you are examining, based on the type of software used to create it.

Training to examine email headers is available to North Carolina law enforcement officers in the course “Fundamentals of Cybercrime Investigation” offered by the North Carolina Justice Academy.

For more information, visit the Academy on the web at WWW.JUS.STATE.NC.US/NCJA

A young woman with dark hair is sitting in the driver's seat of a car. She is wearing a dark zip-up hoodie with white stripes on the sleeves. She is looking out the window to her right with a serious, somewhat somber expression. The car's interior, including the headrest and seatbelt, is visible. The background outside the car shows a blurred view of trees and a road.

Inappropriate use of the Internet can have dangerous consequences for young people

MAKE INTERNET SAFETY PART OF YOUR TEACHING DAY

Internet safety is included in North Carolina's Standard Course of Study for the Computer/Technology Skills and Healthful Living curriculums. K-12 teachers should take advantage of opportunities to reinforce the importance of Internet safety.

You can also reinforce the need for young people to practice Internet safety by inviting a speaker to address your class. A representative from a local law enforcement agency, your district attorney's office, the Attorney General's Office, or a child safety organization can provide real-life examples of how inappropriate use of the Internet can have dangerous consequences for young people.

ncdoj.com



EDUCATORS ARE PARENTS TOO

If you would like information about how to keep your own children safe when they use computers and the Internet, visit WWW.NCDOJ.COM. Under the Jump To menu, select "Internet Safety" and then "Parents and Guardians."

NOTES

NOTES



FOR MORE INFORMATION ABOUT INTERNET SAFETY AT
SCHOOL AND SPECIAL LINKS FOR EDUCATORS, VISIT

ncdoj.com

